Hops: Incorporating exchangable units of USDvalue and Bitcoinvalue in a trustless altcoin

Version 1
September 19, 2013

Cunicula

Abstract

Hop is a proposed PoW/PoS cryptoasset system. Hop aims to facilitate trustless decentralized exchange of convertible equity shares (called hops), USD denominated convertible bonds (called hopdollars), and bitcoin denominated convertible bonds (called hopbits). Bonds are convertible into equity after a 7 month commitment period. Likewise, equity is convertible into either type of bonds after a 7 month commitment period. Conversion ratios are determined 7 months after asset holders commit to a conversion transaction. Hop relies on a global consensus of PoS miners to adjust conversion ratios between hopdollars, hopbits, and hops in reposnse to recent price movements. Unlike other proposed systems for issuance of USD-denominated cryptoassets (e.g. Ripple, Mastercoin, Bitshares, etc.), hop does not rely on trust relationships.

Goals

The goals of hop are the following: facilitate trustless, decentralized exchange of hop equity shares (called hops), USD denominated bonds (called hopdollars), and bitcoin denominated bonds (called hopbits).

Introduction

Hop is a heterodox addition to the cryptocurrency world.

Hop's heterodox features include:

1) Use of PoS miner submitted data to conduct market intervention.

2) Decentralized management of the prices and supply for hopdollars and hopbits

3) No ceiling on the long-term supply of hops

4) Complete pre-mining of the initial supply of hops

5) Potentially large changes in the supply of hops over short time spans (episodes of hyperinflation and hyperdeflation of hops may occur)

6) no protection against erosion in the value of hop equity holdings due to hyperinflation

7) minting of hops, hopdollars, and hopbits through bond conversion txns

8) introduction of a novel PoS mining and voting process

9) Perpetual hop creation via the mining process (target of about 5% inflation; realized levels are highly unpredictable however)

10) imposition of interest/demurrage on hopdollar bond holdings.

I leverage these heterodox properties to facilitate the creation of USD and bitcoin units of value. I have set aside established cryptocurrency principals wherever I feel that this helps me achieve hop's aims. I have many different ideas on how to improve cryptocurrency that are not represnted in hop. I have set aside these ideas to keep hop simple.

User Experience

In many respects, hop operates like other cryptocurrency systems. Users hold a wallet containing three asset types: hops, hopdollars, and hopbits.

Users sign transactions to generate outputs of hops, hopdollars, and hopbits from inputs of hops, hopdollars, and hopbits.

Like bitcoins, hop inputs do not bear interest and are not charged demurrage.

Unlike bitcoins, hopdollar inputs and hopbit inputs accumulate through interest and decay through demurrage.

Hop offers its users the opportunity to exchange units of USD value and bitcion value on a decentralized trustless platform.

Basic Mining Parameters

Two block types are used, type PoS and type PoW. Both block types rely on mixed PoW/PoS mining, but type PoS emphasizes PoS and type PoW emphasizes PoW.

Seperate difficulty levels apply to each block type. Difficulty leves are adjusted to maintain a mean block interval of 7 minutes.

Type PoS and Type PoW blocks are mined in the following deterministic pattern: $PoS\_PoS\_PoW\_PoS\_PoS\_PoW\_PoS\_PoS\_PoW\_...$

Further details on the mining process are deferred to a later version of the paper. This is a very simple component of the paper. I feel that discussion of mininig algorithm's in the first paper version could detract from more important issues.

PoS Miner Voting

Links between hop and real world stem from data submitted by PoS miners. Approximately speaking, the PoS mining algorthim allocates about 80% of mining power in

proportion to coin ownership and 20% of mining power in proportion to hashing power. The specifics of the mining algorithm are treated later.

Each PoS block includes two binary votes, one for hopdollars and one for hopbits.

For hopdollars, miners include a Yes vote if hopdollars current market price is less than 1 USD and a no vote if hopdollars market price is more than 1 USD.

For hopbits, miners include a Yes vote if hopbits current market price is less than 1 bitcoin and a no vote if hopbits market price is less than 1 bitcoin.

Yes votes increase the number of hops backing each hopdollar leading to appreciation of the hopdollar.

No votes decrease the number of hops backing each hopdollar leading to depreciation of the hopdollar.

Likewise for hopbits.

PoS Miners are expected to submit true price reports due to their financial interest in hop's success.

Technical Details (This section provides precise definitions that clarify the system's economic properties. Most readers will want to skim/skip this.)

State Variables

Hop uses state variables to manage the prices and issuance volumes of hopdollars and hopbits.

State variables summarize:

a) rules for determining outputs generated in block h from conversion txn inputs sent in block $h - 40000$.

b) rules for calculating spendable bond outputs in block h from bond inputs received in block x, where $x < h$.

c) Laws of Motion: Rules for calculating state variables at block $h+1$ as a function of block h state variables and data contained in block h and block $h-40000$

State variables used in hop are as follows:
$c_h^{hopbits}$ the current conversion ratio for a hopbit (denominated in hops)
$c_h^{hopdollars}$ the current conversion ratio for a hopbit (denominated in hops)
$g_h^{hopdollars}$ the current per block growth rate in the conversion ratio for hopdollars

$g_h^{hopbits}$ the current per block growth rate in the conversion ratio for hopbits
$\bar{c}_h^{hopbits}$ the average unit conversion ratio for a hopbit (denominated in hops) over the past 8000 blocks
$\bar{c}_h^{hopdollars}$ the average conversion ratio for a hopdollar (denominated in hops) the past 8000 blocks
$q_h^{hops->hopbits}$ the outstanding supply of unspendable hops awaiting conversion into hopbits
$q_h^{hops->hopdollars}$ the outstanding supply of unspendable hops awaiting conversion into hopdollars
$q_h^{hops<-hopbits}$ the outstanding supply of unspendable hopbits awaiting conversion into hops
$q_h^{hops<-hopdollars}$ the outstanding supply of unspendable hopdollars awaiting conversion into hops
q_h^{hops} the outstanding supply of spendable hops
$q_h^{hopbits}$ the outstanding supply of spendable hopbits
$q_h^{hopdollars}$ the outstanding supply of spendable hopdollars
$\{r_{h+1,x}^{hopdollars}\}$ where $x = 1, ..., h$. Interest adjustment factor converting hopdollar inputs received in block x to spendable hopdollar outputs in block $h+1$.
$\{r_{h+1,x}^{hopbits}\}$ where $x = 1, ..., h$. Interest adjustment factor converting hopbit inputs received in block x to spendable hopbit inputs in block $h+1$.

Novel data included in block h and data carried over from block $h-40000$ that enter in to state variable laws of motion:
$v_h^{hopbits}$ a binary vote equal to either 1 or -1 in a PoS block and 0 in PoW block. The vote influences $g_{h+1}^{hopbits}$
$v_h^{hopdollars}$ a binary vote equal to either 1 or -1 in a PoS block and 0 in PoW block. The vote influences $g_{h+1}^{hopdollars}$
$s_h^{hops->hopbits}$ the sum of hop inputs in block h conversion transactions that convert hops into future hopbits
$s_h^{hops->hopdollars}$ the sum of hop inputs in block h conversion transactions that convert hops into future hopdollars

$s_h^{hops<-hopbits}$ the sum of hopbit inputs in block h conversion transactions that convert hopbits into future hops

$s_h^{hops<-hopdollars}$ the sum of hopdollar inputs in block h conversion transactions that convert hopbits into future hops

$s_{h-40000}^{hops->hopbits}$ the sum of hop inputs in block h conversion transactions that convert hops into future hopbits

$s_{h-40000}^{hops->hopdollars}$ the sum of hop inputs in block h conversion transactions that convert hops into future hopdollars

$s_{h-40000}^{hops<-hopbits}$ the sum of hopbit inputs in block h conversion transactions that convert hopbits into future hops

$s_{h-40000}^{hops<-hopdollars}$ the sum of hopdollar inputs in block h conversion transactions that convert hopbits into future hops

Laws of Motion:

$$g_{h+1}^{hopbits} = \max\left(-1, g_h^{hopbits} + 3\left(10^{-7}\right)v_h^{hopbits}\right)$$

$$g_{h+1}^{hopdollars} = \max\left(-1, g_h^{hopdollars} + 3\left(10^{-7}\right)v_h^{hopdollars}\right)$$

$$c_{h+1}^{hopbits} = (1 + g_h^{hopbits})c_h^{hopbits}$$

$$c_{h+1}^{hopdollars} = \left(1 + g_h^{hopdollars}\right)c_h^{hopdollars}$$

$$\bar{c}_{h+1}^{hopbits} = \frac{1}{8000}c_h^{hopbits} + \frac{7999}{8000}\bar{c}_h^{hopbits}$$

$$\bar{c}_{h+1}^{hopdollars} = \frac{1}{8000}c_h^{hopdollars} + \frac{7999}{8000}\bar{c}_h^{hopdollars}$$

$$q_{h+1}^{hops->hopbits} = q_h^{hops->hopbits} + s_h^{hops->hopbits} - s_{h-40000}^{hops->hopbits}$$

$$q_{h+1}^{hops<-hopbits} = q_h^{hops<-hopbits} + s_h^{hops<-hopbits} - s_{h-40000}^{hops<-hopbits}$$

$$q_{h+1}^{hops->hopbdollars} = q_h^{hops->hopdollars} + s_h^{hops->hopdollars} - s_{h-40000}^{hops->hopdollars}$$

$$q_{h+1}^{hops<-hopdollars} = q_h^{hops<-hopdollars} + s_h^{hops<-hopdollars} - s_{h-40000}^{hops<-hopdollars}$$

$$q_{h+1}^{hops} = \left(1 + 3\left(10^{-7}\right)\right)(q_h^{hops} + s_{h-40000}^{hops<-hopbits}\bar{c}_h^{hopbits} + s_{h-40000}^{hops<-hopdollars}\bar{c}_h^{hopdollars} - s_h^{hops->hopdollars} - s_h^{hops->hopbits})$$

$$q_{h+1}^{hopdollars} = r_{h+1,h}^{hopdollars}(q_h^{hopdollars} + r_{h,h-40000}^{hopdollars}s_{h-40000}^{hops->hopdollars}\left(\bar{c}_h^{hopdollars}\right)^{-1} - s_h^{hopdollars->hops})$$

$$q_{h+1}^{hopbits} = r_{h+1,h}^{hopbits}(q_h^{hopbits} + r_{h,h-40000}^{hopbits}s_{h-40000}^{hops->hopbits}\left(\bar{c}_h^{hopdollars}\right)^{-1} - s_h^{hopbits->hops})$$

$$V_h^{hopdollars} \equiv 100\frac{q_h^{hopdollars}\bar{c}_h^{hopdollars} + q_h^{hops->hopdollars}}{q_h^{hopdollars}\bar{c}_h^{hopdollars} + q_h^{hops->hopdollars} + q_h^{hops} + q_h^{hops<-hopdollars}\left(\bar{c}_h^{hopdollars}\right)^{-1} + q_{h+1}^{hops<-hopbits}\bigl(\bar{c}_h^{hopbits}}$$

$$V_h^{hopbits} \equiv 100\frac{q_h^{hopbits}\bar{c}_h^{hopbits} + q_h^{hops->hopbits}}{q_h^{hopbits}\bar{c}_h^{hopbits} + q_h^{hops->hopbits} + q_h^{hops} + q_h^{hops<-hopdollars}\left(\bar{c}_h^{hopdollars}\right)^{-1} + q_{h+1}^{hops<-hopbits}\left(\bar{c}_h^{hopbits}\right)^{-1}}$$

$$r_{h+2,h+1}^{hopdollars} = \begin{array}{ll} \left(1 + \left(10^{-5}\right)\min\left(1, \frac{1}{4}\left(\ln V_h^{hopdollars}\right)^4\right)\right) & \text{if } V_h^{hopdollars} < 1 \\ \left(1 - \left(10^{-5}\right)\min\left(1, \frac{1}{4}\left(\ln V_h^{hopdollars}\right)^4\right)\right) & \text{if } V_h^{hopdollars} > 1 \end{array}$$

$$r^{hopbits}_{h+2,h+1} = \begin{matrix} \left(1 + \left(10^{-5}\right) \min\left(1, \frac{1}{4}\left(\ln 2 + \ln V^{hopbits}_{h}\right)^{4}\right)\right) & \text{if } V^{hopbits}_{h} < \frac{1}{2} \\ \left(1 - \left(10^{-5}\right) \min\left(1, \frac{1}{4}\left(\ln 2 + \ln V^{hopbits}_{h}\right)^{4}\right)\right) & \text{if } V^{hopbits}_{h} > \frac{1}{2} \end{matrix}$$

$$r^{hopdollars}_{h+2,x} = r^{hopdollars}_{h+2,h+1}\left(r^{hopdollars}_{h+1,x}\right) \text{ for all } x = 1, ..., h$$

$$r^{hopbits}_{h+2,x} = r^{hopbits}_{h+2,h+1}\left(r^{hopbits}_{h+1,x}\right) \text{ for all } x = 1, ..., h$$

Txns rules

Excluding hop to hop txns, all txns are designated with a specific block height and are only valid txns if they are included in a block that matches this height.

$Hops- > Hops$

Rules are identical to bitcoin inputs = outputs + fees for all blocks

$Hopbits- > Hopbits$

a hobit inputs received in block x generate $r^{hopbits}_{h+1,x}a$ spendable outputs in block $h+1$ (i.e. $r_{h+1,x}$(inputs)=ouputs+fees in block $h+1$

$Hopdollars- > Hopdollars$

a hobit inputs received in block x generate $r^{hopdollars}_{h+1,x}a$ spendable outputs in block $h+1$

$Hopbits- > Hops$

a hopbit inputs txn in block $h - 40000$ generate $a\bar{c}^{hopbits}_{h}$ spendable hops in blocks $h+1$ and onwards

$Hopbits < -Hops$

a hop inputs txn in block $h - 40000$ generate $ar^{hopbits}_{h+1,h-40000}\left(\bar{c}^{hopbits}_{h}\right)^{-1}$ spendable hopbits in blocks $h+1$ and onwards

$Hopdollars- > Hops$

a hopdollar inputs txn in block $h - 40000$ generate $a\bar{c}^{hopdollars}_{h}$ spendable hopdollars in blocks $h+1$ and onwards

$Hopdollars < -Hops$

a hop inputs txn in block $h-40000$ generate $ar^{hopdollars}_{h+1,h-40000}\left(\bar{c}^{hops}_{h}\right)^{-1}$ spendable hopdollars in blocks $h+1$ and onwards

Economic Implications of System

Incentives for PoS Miners

The value of hopdollars and hopbits is backed by an option to convert these bonds into hops at a conversion rate determined 4 to 7 months in the future. The conversion rate for both bonds adjusts so that the market prices of hopdollars and hopbits track the market prices of real world USD and bitcoin. Adjustments to the conversion rate are based on data input into the blockchain. PoS miners submit these data as they mine blocks. PoS miners are expected to report accurate data due to their financial stake in Hop's success. By submitting accurate data PoS miners can ensure that 1 hopdollar trades for 1 USD and 1 hopbit trades for 1 bitcoin except under extraordinary circumstances.

Mechanism Deteming $Hopdollar$ and $Hopbit$ Prices: Arbitrage Conditions for Debt <-> Equity Conversion

Let $p_h^{hopdollar}$ be the value of price of a hopdollar in terms of hops at blockheight h.

Let $\rho_{h,h+40000}^{hopdollars}$ be the appreciatoin of hopdollars in terms of hops between time h and time $h + 40000$

Consider two different investment strategies that seek to maximize return in hops:

A user can buy and hold hopdollars, hops, or convert between hopdollars and hopbits.

It is weakly optimal to convert a hopdollar to equity iff

$$E_h\left[\bar{c}_{h+40000}^{hopdollars} - r_{h+1,h-40000}^{hopdollars}\rho_{h+1,h+40000}^{hopdollars}\right] \geq 0$$

Likewise it is weakly optimal to convert a hop to a hop dollar iff

$$E_h\left[\bar{c}_{h+40000}^{hopdollars} - r_{h+1,h-40000}^{hopdollars}\rho_{h+1,h+40000}^{hopdollars}\right] \leq 0$$

In equilibrium, people must always voluntarily hold both hops and hopdollars. This implies

$$E_h\left[\bar{c}_{h+40000}^{hopdollars} - r_{h+1,h-40000}^{hopdollars}\rho_{h+1,h+40000}^{hopdollars}\right] = 0$$

Note that $r_{h+1,h-40000}^{hopdollars}$ depends on how people respond to demurrage / interest incentives. As I discuss in the next section,

the term $r_{h+1,h-40000}^{hopdollars}$ is unlikely to deviate very far from 1. Thus it can be neglected for simplicity.

$E_h\left[\bar{c}_{h+40000}^{hopdollars} - \rho_{h+1,h+40000}^{hopdollars}\right] = 0$

What this tells us is that changes in the relative prices of hops and hopdollars are completely dependent on $E_h\left[\bar{c}_{h+40000}^{hopdollars}\right]$

As long users expect PoS miners to vote honestly. They will expect adjustments in $\bar{c}^{hopdollars}_{h+40000}$ that ensure that the hopdollar maintains parity with one real USD.

If PoS miners have made these adjustments in the past, users are likely to expect them to continue to do so in the future.

The same logic maintains parity between 1 hop bit and 1 bitcoin.

Regulating Bond Supply: Interest and Demurrage Enhance the Hop System Sustainability

Use of hopbits and hopdollars as a long-term store of value imposes systemic risk on the hop financial system. Hops are equity and hopbits and hopdollars are bond liabilities. When bitcoins or dollars appreciate relative to hops, the ratio of debt value to equity value (leverage) increases. Overleveraging could cause the hop system to collapse catostrophically. To avoid this, hop uses interest and demurrage to target a 200 fold ratio of hop equity value to bitcoin debt and a 100 fold ratio of hop equity value to USD debt. These extremely conservative leverage ratios allow hop to withstand extremely large price shocks without generating a risk of collapse. When leverage becomes excessive, demurrage imposes a financial penalty on long-term storage of value in hopbits and hopdollars. Conversions to equity reduce leverage in the system. In the aggregate, demurrage encourages users to convert hopbits and hopdollars into hops. Immediate conversion allows the converting user to escape all demurrage penalties. Once leverage falls to the target ratio, demurrage is no longer charged on hopbit and hopdollar holdings. Accordingly, conversions also have spillover effects, allowing other users to escape demurrage penalties as well. Due to the ease of escaping demurrage and the consequences of this for other users, it unlikely that users will see long-term demurrage rates that differ significantly from 0%. For very short periods, (likely less than a day), however, annualized demurrage may be substantial. When hop appreciates relative to bonds, leverage in the system decreases. This allows the system to safely store additional value in hopbits and hopdollars. Gains from hop appreciation are potentially shared among holders of hopbits and hopdollars through interest payments. However, as for demurrage, interest payments are immediately available to all system users through conversions. Just as these conversoins will keep long-term demurrage rates close to 0%, they will also prevent assets from persistently offering substantial interest. Again, however, for very short peroids, annualized interest rates may be substantial.

The net consequence of this system is to force the system to maintain a 200 fold ratio of hop equity value to bitcoin debt and a 100 fold ratio of hop equity value to USD debt. Without demurrage penalties, the system could easily become overleveraged and face a risk of sudden crises.

Comments

Hop is really a kind of decentralized bank or payment intermediary. People will use hops, hopbits, and hopdollars to make speculate and make payments.

Hop holders earn fees from this by PoS mining. They are also tasked with critical decisions that manage the hop system. The rate of return for hop holders

depends on leverage. Banks are always tempted to increase leverage because that enables them to earn more fees/interest relative to the capital invested.

The more leverage, the higher the average return on assets. This would also apply to hop holders. They could earn more in fees per hop with higher leverage ratios.

High leverage however leads to frequent banking faliures. I have imposed draconian constraints on leverage via the demurrage system. I think avoiding instability is much more important than maximizing short-run efficiency. This is why demurrage is necessary for debt holders.